Department of Administrative Services

April 2004

OPERATING SECURITY POLICY

General Principles: (April 2004)

Networked computer systems are increasing in number, capability, and importance. At the same time, threats to those systems are increasing in number and sophistication. As a result of these two factors, an emphasis on information security is necessary to protect these systems and the information they store and process. The Government of the State of Iowa is working towards providing greater access, more information, and new services to State employees and citizens. As these capabilities increase, security becomes even more important. Information security encompasses several areas, including computer, communication, and physical security disciplines. The Department of Administrative Services (DAS) has instituted this operating security policy to enhance the DAS security posture and support State information security efforts. Compliance with this policy is mandatory for all DAS employees and contractors. Non-compliance may result in appropriate disciplinary actions up to and including immediate dismissal. Criminal and/or civil action against users may be appropriate where laws are violated. Where this policy differs with other established policy statements, the more current policy by date shall be enforced.

DAS management is required to:

1) Provide clear policies, procedures, and guidelines to DAS employees.
2) Provide security training on an annual basis.
3) Provide each employee a picture identification badge.

At a minimum, DAS employees shall:

1) Know, understand, and follow this operating security policy.
2) Safeguard State computer resources, sensitive or otherwise confidential information, and Government buildings and property.
3) Attend security training on an annual basis.
4) Wear their ID badge or a temporary badge when in DAS facilities.
5) Follow all federal and state laws that apply to computers, networks, and electronic communication.

Specific Policy Statements

1) Security Training
    a) DAS employees and contractors shall attend security training on an annual basis.
    b) Security training shall be accomplished prior to receiving system access.
    c) Initial training will be provided by a quarterly briefing. Newly gained employees shall initially view the training videotape and also attend the next scheduled training session.
    d) Annual refresher training shall be accomplished via computer based training every January.

e) Users who do not complete the annual refresher training shall have their network privileges revoked.

f) An acknowledgment form shall be signed by each employee and contractor after each training session indicating training was received and understood.

2) Physical Security

a) All doors to DAS that are required to be locked shall be locked at all times.

b) Each employee and long-term contractor shall be issued a key card allowing access to DAS facilities. Access requirements shall be determined by the supervisor and key card monitors.

c) Employees and contractors shall not admit other people to DAS facilities unless they display a valid DAS picture or temporary badge.

d) Non-DAS State personnel displaying State issued ID badges shall be considered visitors.

e) Doors shall not be propped open unless the entryway remains controlled.

f) The door to the vault containing warrants shall be locked at all times. When entrance is necessary, the operator shall be accompanied by the manager, supervisor, or senior operator in charge.

g) The daily security checklist shall be completed nightly on the south side of DAS Hoover facilities.

h) Personnel working after business hours shall not enter offices or areas where access is not essential to complete their duties.

i) Employees and contractors are responsible for safeguarding State computer resources, sensitive or confidential information, and Government buildings and property.

3) Identification Badges

a) DAS employees and long-term contractors shall wear their State supplied picture identification badge at all times while in DAS facilities.

1) The badge shall be worn between the waist and shoulders, with the picture or temporary indicator plainly visible and right side up.

2) If an employee forgets their badge, they shall sign in at the receptionist's desk and wear a temporary badge for that day.

3) Temporary badges shall be returned at the end of the day.

4) Personal and temporary badges shall be safeguarded by each employee.

b) Visitors shall be required to wear a visitor's badge while in DAS facilities.

1) Each visitor shall sign in and receive a visitor's badge at the receptionist's desk.

2) Each visitor shall be escorted at all times while on DAS premises by an DAS employee. Each escort is responsible for the conduct and whereabouts of their visitors.

3) The badge shall be worn between the waist and shoulders, with the visitor indicator plainly visible and right side up.

4) The badge issuing employee shall be responsible for instructing visitors on DAS security guidelines and how to wear the badge.

5) Each visitor shall sign out and return their visitor's badge prior to departing DAS facilities.

4) Unattended Terminals

a) Users shall lock their workstations when leaving the vicinity of their desk.

b) A password protected screensaver shall be enabled on each workstation, with the time set to no more than 15 minutes of inactivity.

c) Users shall log out of their workstations at the end of each day, unless they have a valid operational reason for leaving them logged on. If left logged on, the workstation shall be locked. Once logged out, the workstation shall be shut off.

5) Consent to Monitoring

a) Use of State Government computer systems implies consent to monitoring of that usage by the Director and specific designees.

b) The State of Iowa Employee Handbook's "Management Access to Work Areas" section identifies computer data and information as materials and tools to be used for work-related purposes only. As such, management has the right of access to these work areas. For more information, see the DAS Work Rules.

c) Any monitoring shall be in compliance with Iowa Code Chapter 22.

6) Use of State Computers

a) Users shall abide by the policy statements contained in the DAS Work Rules, and contained in the DAS Work Rules.

b) State computers shall not be used for:

1) Access to, use, or distribution of material that:

a. Is deemed obscene by a reasonable person, or

b. Would contribute to a hostile environment;

2) Seeking out unauthorized information which is private, confidential, or not open to the public;

3) Any purpose which violates US or State of Iowa law, specifically, but not limited to, Iowa Code Chapter 22; or

c) Personal use of government computers is authorized on a limited basis as long as it does not disrupt operations, detract from work tasks, or otherwise violate DAS policy.

d) Managers shall be responsible for the security and proper use of computer hardware, software, and data within their areas.

e) Managers shall be responsible for ensuring their staff has been adequately trained in basic security concepts and are aware of the policies, procedures, and guidelines concerning their use and security.

f) Computers shall not be installed, moved, removed, or connected to the network without coordinating with the Help Desk.

7) Internet Use

a) Users shall abide by the policy statements contained in the DAS Internet and Email Usage, contained in the DAS Work Rules.

b) Users shall not:

1) Violate laws;
2) Interfere with network users, services, or equipment; or
3) Harass other users.

c) Personal Internet use is authorized on a limited basis as long as it does not disrupt operations, detract from work tasks, or otherwise violate DAS policy.

8) E-mail

a) Users shall abide by the policy statements contained in the DAS Internet and Email Usage Policy contained in the DAS Work Rules.

b) E-mail shall not be considered private and protected unless encrypted. Confidential or sensitive information shall not be e-mailed. It is the sender's responsibility to determine the confidentiality of each e-mail sent.

c) E-mail received that is of a questionable nature (unusual attachment, not expected, similar e-mails received, etc.) should not be opened. If there is any question as to the validity of an e-mail received, contact DAS Security.

d) Occasional e-mail of a personal nature may be sent and received as long as it does not disrupt operations, detract from work tasks, or otherwise violate DAS policy.

9) Software

a) Users shall abide by the policy statements contained in the DAS Internet and Email Usage Policy, contained in the DAS Employee Handbook.

b) Shareware and freeware from any source shall be installed only with management approval.

c) Software installation shall be coordinated with the Help Desk.

d) Approved software shall be scanned for viruses prior to installation.

10) Anti-virus Software

a) All desktop and portable computers shall have current anti-virus software installed.

c) Users shall not change anti-virus software settings or otherwise interfere with the functioning of the software unless directed by a system or security administrator.

d) Users shall make every attempt to limit exposure to a virus or other malicious software.

11) User IDs

a) User IDs no longer required shall be deleted.

b) Managers shall ensure that accounts are deleted as necessary.

1) For the DAS LAN, accounts shall be deleted when a user terminates State employment, transfers to a different department, or no longer needs access. Accounts shall be deleted within 24 hours of departure.

2) TSO ID: If a user transfers to a different department, terminates state employment, or no longer requires an account, their TSO ID shall be disabled and information associated with the account shall be retained. If a request has

not been made within 30 days by the department to retain the ID and associated datasets, the account and associated information shall be deleted.

c) Accounts shall be locked for a period of 24 hours after 3 login failures. Authorized users may have their accounts reset immediately by contacting the Help Desk.

12) Passwords

a) Passwords for DAS computer systems and networks shall be:

1) A minimum of 8 alphanumeric characters with at least one special character;

2) Upper and lower case, if the system allows it;

3) Changed at least every 60 days with no repetitions; and

4) Protected at the highest level of information on the system.

b) Default, initial, and system passwords shall be changed immediately upon receipt.

c) Passwords for DAS computer systems and networks shall not be:

1) Written down or recorded on-line in any form;

2) Shared with anybody;

3) Words, or combinations of words, found in dictionaries, spelling lists, or other lists of words, even if combined with other alphanumeric and special characters;

4) A user ID in any form;

5) All digits or all the same letter;

6) Published examples of good passwords;

7) Information easily obtained about the user; or

8) Reused at any time.

d) Certain passwords may be shared and/or written down, with management approval, in order to meet mission requirements. If a password is written down, it shall be stored and protected at an alternate location.

e) Passwords may be set as non-expiring in certain circumstances when other security controls are put in place as compensation. These instances shall be approved on a case by case basis by DAS Security and the administrator involved. Other organizations affected by the decision shall be consulted and afforded the opportunity to provide input. This deviation from policy shall be justified and documented on a waiver form available from DAS Security.

3) Modems

a) Modems on individual computers connected to analog lines shall set auto-answer to off.

b) If a modem is required for business reasons, its use shall be coordinated with DAS Security.

14) Phone/Wiring Closets

a) Phone/wiring closets shall be locked at all times.

b) Access to such closets shall be restricted to those who require it for business or

maintenance purposes.

15) Hardcopy Information

a) Information in hardcopy form that is sensitive or confidential shall be shredded or otherwise destroyed when disposed.

b) It is the employee's responsibility to determine the sensitivity or confidential nature of the information. If unsure, the employee should destroy the information.

16) Bomb Threat Aid

a) A Bomb Threat Card provided by DAS Security shall be kept near each phone in DAS facilities.

b) If a bomb threat is received via telephone, follow the instructions and guidelines on the Bomb Threat Card and answer the questions as accurately as possible.

c) If a bomb threat is received via other means, such as e-mail or postal mail, contact Iowa State Patrol Post 16 immediately.